Kalpana Srinivasan
State Bar No. 237460
Davida Brook
State Bar No. 275370
Susman Godfrey L.L.P.
1900 Avenue Of The Stars, 14th Floor
Los Angeles, California 90067-6029
Telephone: (310) 789-3100
Fax: (310) 789-3150
ksrinivasan@susmangodfrey.com
dbrook@susmangodfrey.com

[Additional Counsel on Signature Page]

Attorneys for Cortex MCP., Inc.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

CORTEX MCP, INC.,

Plaintiff,

v.

VISA, INC.

Defendant.

CASE NO. 5:23-CV-05720-EJD

PLAINTIFF CORTEX MCP, INC.'S OPPOSITION TO DEFENDANT VISA INC.'S MOTION TO DISMISS UNDER FED. R. CIV. P. 12(B)(6) FOR UNPATENTABILITY UNDER SECTION 101 AND TO DISMISS WILLFUL AND INDIRECT INFRINGEMENT CLAIMS

Hearing Date: February 29, 2024
Hearing Time: 9:00 a.m.
Courtroom: Time: 4, 5th Floor.
Judge: Hon. Edward J. Davila

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Other Authorities

INTRODUCTION

Visa, now on its third motion to dismiss, claims *for the first time* that Cortex's claims are not patent eligible. This new argument rests on a mischaracterization of the patents and an improper attempt to reduce Cortex's claims to the purported abstract idea of "issuing and checking credentials," Mot. at 1, 9. Ignoring the patents' narrowly tailored application to electronic transactions on mobile devices and the inventiveness of replacing the sensitive information in user credentials with a secondary representative credential, Visa cannot overcome the patents' presumption of validity—let alone by clear and convincing evidence. Visa's failure is no surprise, as its new claims of ineligibility cannot be reconciled with its own willful adoption of Cortex's technology for its Visa Token Service or with Visa's filing of a patent application for a substantially similar tokenization method. Visa's new claims are also contradicted by binding precedent that inventions like Cortex's, which are focused on a "specific asserted improvement in computer capabilities," *Packet Intelligence LLC v. NetScout Systems, Inc.*, 965 F.3d 1299, 1309 (Fed. Cir. 2020) (cleaned up), are eligible under Section 101. Visa's motion should be denied.

Cortex's family of patents describes a novel method for storing digital credentials and enabling secure digital transactions on mobile devices. Cortex's key innovation is the generation of an electronic representation of a user credential, such as a credit card, that is verifiable through a remote database that is unconnected with the agency that issued the credential. This officially verifiable electronic representation, or OVER File, replaces the sensitive data (i.e., a credit card or drivers' license number) in a user credential with a unique secondary credential that contains no such sensitive data. OVER Files can be stored on user's smartphones, scanned by third parties (such as merchants accepting payment), and verified by issuing agencies (such as banks). Cortex's methods rout all point-of-sale communications through a remote database, the OVER Engine, obviating the need for users *or* merchants to communicate with the agency that issued the underlying credential. Conducting transactions with an OVER File—which has no exploitable meaning or value outside of the OVER File system and —eliminates the risk of identity theft or fraud in electronic transactions, bolstering trust and heightening security.

Cortex's method for secure electronic transactions provides a technological solution to at least two technological problems that hampered the adoption of mobile payments. *See, e.g.*, Compl. ¶¶ 1, 8-9. Specifically, in December 2012, when Cortex submitted the application for its flagship '531 patent, mobile-payment systems were both fragmented and insecure. Existing mobile-payment applications required users to install specialized hardware on their phones to protect against fraud in transactions involving the transmission of personal data. *Id.* ¶ 8. Implementation of these applications required merchants to purchase specialized hardware. *Id.* Cortex's invention eliminates all the difficulties inherent to previous approaches—by creating a system for storing and verifying credentials that does not involve the transmission of sensitive information and that is compatible with both major smartphones and existing point-of-sale infrastructure. *Id.* ¶¶ 8-9. Both Visa and its customers benefit from the increased digital security, and resilience against would-be hacks, of the OVER File system.

Visa has been fully aware of the utility and inventiveness of Cortex's methods long before Cortex brought this action. In April 2016, Visa reached out to Cortex seeking information on how the OVER File could be applied to its payment business. *Id.* ¶ 11. On two separate occasions, Shaunt Sarkissian, Cortex's Chief Executive Officer and the inventor of the OVER File system, provided Visa with a detailed description of the patented technology, an explanation of how Visa could incorporate its technology, and a caution that Cortex's intellectual property was subject to infringement from existing wallet solution providers. *Id.* After receiving that information, Visa sold and promoted products, including the Visa Token Service, that practice the methods patented by Cortex. Visa now touts its token service as "the foundational platform for global tokenization," and claims that "substituting Visa card numbers with tokens … enables richer, more secure digital payment experiences for millions of customers every day."[1] In reality, Visa's "token" is simply another word for Cortex's OVER File. And the teachings of Cortex's patents are now widely adopted in mobile-payment systems, including the Visa Token Service.

[1] https://usa.visa.com/products/visa-token-service.html.

FACTUAL BACKGROUND

I. Cortex's Patents

Cortex asserts four related patents, each titled "File Format and Platform for Storage and Verification of Credentials": United States Patent Nos. 9,251,531 ("'531 Patent"); 9,954,854 ("'854 Patent"); 10,749,859 ("'859 Patent"); and 11,329,973 ("'973 Patent") (collectively, the "Asserted Patents"). The Asserted Patents share a common specification and generally relate to a system, method, and apparatus for the use of electronic representations of credentials on mobile devices. Cortex contends that Visa infringes at least claim 1 of the '531, '859, and '973 patents, and claim 15 of the '854 Patent (the "Asserted Claims"). *See* Compl. ¶¶ 16, 37, 60, 80.

Independent claim 1 of the '531 Patent is representative of the Asserted Claims and teaches a comprehensive method for the generation, storage, transmission, and verification of a virtual representation of a user credential. As explained in the specification, Cortex's innovation lies in the use of a virtual representation of the credential, rather than the credential itself, thereby providing "a secure file format and platform for the storage and verification of key user or consumer credentials." '531 Patent at 4:50-43. Specifically, an OVER File is a *secondary* credential that permits verification of the user's primary credential but contains none of the sensitive information contained therein. The system thus allows for digital credentials to be stored on user's smartphones and verified by third parties without exposing sensitive information *or* requiring communication with the issuing agency. Claim 1 recites each aspect of this system.

The first limitation of Claim 1 comprises "storing, in a memory of an officially verifiable electronic representation (OVER) generation and verification engine, information associated with a credential of a user for proving the user's identity or qualifications." *Id.* at 21:15-19. This OVER File generation and verification engine is a remote server that securely stores the sensitive information contained in a user credential. *Id.* at 4:12-15. As described in the second and third limitations, the OVER engine generates a virtual representation of the credential that has been verified by the issuing agency in response to a request from a user device. *Id.* at 21:20-28. The engine then transmits this virtual representation to the user device where it is stored as an OVER File—a replacement for the user's credential. *Id.* at 21:29-31. When a third party scans the OVER

File stored on the user device, a verifying request is sent to the OVER engine. *Id.* at 21:32-36. The OVER engine then verifies that the scanned OVER File corresponds to the user's underlying credential and transmits to the third-party device a message confirming the user's credentials. *Id.* at 21:37-46. In sum, Claim 1 permits users to conduct electronic transactions, like credit-card payments, without having to transmit any sensitive information. Both the user requesting verification and the third-party seeking verification can use the same OVER File system without having to directly contact the agency that issued the credential. Independent claim 21 is an apparatus claim with similar limitations. *Id.* at 23:27-24:4.

The dependent claims of the '531 patent provide additional security innovations to the OVER File system. For example, Claim 4 recites a method by which the OVER Engine communicates with the issuing agency to ensure that the user credential is, and remains, valid. If a user credential is invalid, Claim 7 recites a method by which the issuing agency—through the OVER Engine—indicates the reason for the invalid credential to the third-party requestor. Claim 15 recites a method in which a third-party can scan a portion of the OVER File displayed on a client device to authenticate the user. And Claim 17 provides a method in which the OVER File's validity is limited to a particular device of a particular user. These limitations prevent someone who illicitly obtains an OVER File from either accessing the user's personal information, using her credentials, or utilizing her device in mobile transactions.

Adding another layer of complexity, the '854 patent describes a method for generating multiple OVER Files that are tied to the same underlying credential. This allows a user to securely authenticate multiple devices for use based on the same original credential of the user, without sacrificing efficiency. As described in Claim 15, the additional OVER File, which is a second virtual representation of the original user credential that has been verified by the issuing agency, is specific to a particular user device and "invalid for use in the first OVER file client device." '854 patent at 24:34-44. Tying each (or in the context of Claim 15, both) OVER file(s) to a specific device increases security as a compromised OVER File can be easily revoked and regenerated.

The purpose of this novel and inventive method is explained in the patent itself:

"[C]urrently payment systems are highly fragmented and insecure, which creates a threat of data compromise and theft during the transfer and use of electronic commerce data. This threat may result in losses for corporations as well as users of such systems, and these losses factor into escalating fees and client costs…. Current platforms are insecure and carrying digital credentials increases the risk of identity theft or fraud in transactions. What is needed is [a] secure system for storing and displaying user credentials." *Id.* at 1:26-39. The Asserted Patents disclose a one-of-a-kind secure and user-friendly system for storing and verifying credentials in a virtual wallet. They create a flexible interoperable platform with no ties to specific hardware or brands.

II. Visa's Pre-Suit Knowledge of the '531 Patent

Cortex and Visa engaged in extensive pre-suit discussions about the '531 Patent and its relation to the Visa Token Service. As alleged in Cortex's Complaint, Visa first learned of Cortex's OVER File technology within seven months of Cortex's application for the '531 Patent. *See* Compl. ¶¶ 1, 10. Specifically, in a July 2013 meeting with Visa-subsidiary CyberSource, Cortex representatives presented the OVER File platform and explained the underlying technology that is reflected in the '531 Patent. *Id.* ¶ 10. Notably, the parties were meeting to explore a business relationship that would merge Cortex's OVER File technology with Visa's mobile-commerce business. *Id.* Cortex informed CyberSource that it had filed a patent application for the technology presented and explained how that technology would be useful for Visa's business. *Id.* On February 2, 2016, the U.S. Patent & Trademark Office granted Cortex the patent application discussed in the July 2013 meeting. *Id.* ¶ 13, Ex. 1.

In April 2016, approximately two months after the issuance of the '531 Patent, Visa requested additional information from Cortex about a potential business relationship. *Id.* ¶ 11. Shaunt Sarkissian, Cortex's Founder and CEO and the inventor of the '531 Patent, communicated directly with Jim McCarthy, Visa's Head of Innovation and the man responsible for the introduction of the Visa Token Service. *Id.* Mr. Sarkissian sent Mr. McCarthy two documents that described the OVER File technology: 1) an outline of Cortex's technologies and their potential

application to Visa's Digital Enablement Program;[2] and 2) a summary of "potential synergies" between Cortex and Visa specifically related to the Visa Token Service. *Id.* These documents explained Cortex's OVER File technology, and expressly stated that Cortex had been issued "an OVER File patent." *Id.* Cortex also explained the scope of the OVER File IP as "covering every aspect of provisioning a representative credential, that can be scanned and verified," and alerted Visa that the OVER File IP was subject to "exi[s]ting infringement from most all Wallet Solution providers." *Id.* Both documents described the connection between the OVER File IP and the Visa Token Service. For example, the first document represented that Cortex's "[t]okenization capabilities can add significant value, IP, and capacities to the Visa Token Service," while the second stated that Cortex's technology could provide a "[c]ritical supporting IP portfolio" for the Visa Token Service. *Id.* In early 2017, Mr. Sarkissian again emailed the same information—describing the OVER File technology and citing the OVER File patent—to Visa Executive Vice President William Sheedy. *Id.* Based upon the foregoing, Cortex has sufficiently alleged that Visa has known of the '531 Patent and the infringing nature of the Visa Token Service since at least April 2016 to sustain the willful and indirect infringement claims. *Id.* ¶ 26.

III. Visa's Provision of Support, Encouragement, and Instructions on Infringement

The Complaint also contains specific allegations about the ways in which Visa directs third parties—banks, retailers, developers, and end users—to use the Visa Token Service in an infringing mode. Through EMVCo, Visa publishes a payment tokenization "Specification Framework" and "Guide to Use Cases," each of which provides detailed instructions on how to implement an infringing tokenization service. Compl. ¶¶ 27, 50, 70, 93. The stated purpose of these documents is to "support adoption" of tokenization, *i.e.*, infringing products. *See id.* ¶ 27. Recognizing that implementation of the use guide may infringe the patent rights of third parties, EMVCo begins its instructions with a disclaimer. *Id.* Through CyberSource, Visa offers detailed instructions to developers to implement infringing tokenization services. *Id.* Visa also operates a

[2] The Visa Digital Enablement Program is a program that "connects financial institutions and technology companies," including through "access to Visa Token Service." https://ma.visamiddleeast.com/en_MA/partner-with-us/payment-technology/visa-token-service.html.

developer center, which provides software, instructions, and tutorials on how to implement the Visa Token Service, specifically targeted towards issuer banks, merchants, and developers. *Id.* Visa, including through EMVCo and CyberSource, encourages these third parties as well as end users to adopt infringing services by touting the benefits of tokenization. *Id.* The Complaint accompanies these allegations with links to, and direct quotes from Visa's and its affiliates' websites and instructional manuals. *Id.* Such is legally adequate to support Cortex's indirect infringement claims at the pleadings stage.

LEGAL STANDARD

To survive a motion to dismiss, a "complaint must plead enough factual matter, that when taken as true, states a claim to relief that is plausible on its face." *In re Bill of Lading Transmission & Processing Sys. Patent Litig.*, 681 F.3d 1323, 1331 (Fed. Cir. 2012) (cleaned up). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A plaintiff need not "prove its case at the pleading stage." *In re Bill of Lading,* 681 F.3d at 1339. The Court may not "choose among competing inferences as long as there are sufficient facts alleged to render the non-movant's asserted inferences plausible." *Id.* at 1340.

ARGUMENT

I. The OVER File System Is Patent Eligible.

Section 101 broadly provides for the patentability of "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. The Supreme Court has interpreted Section 101 to contain three narrowly construed exceptions: "Laws of nature, natural phenomena, and abstract ideas are not patentable." *Alice Corp. v. CLS Bank International*, 573 U.S. 208, 216 (2014). Under *Alice*'s two-step inquiry, the Court first "determine[s] whether the claims at issue are directed to one of those patent-ineligible concepts," such as an abstract idea. *Id.* at 217. If the answer is no, the inquiry ends and the claims are patent eligible. *See, e.g.*, *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299, 1306 (Fed. Cir. 2018). If the answer is yes, the Court proceeds to "consider the elements of each claim

both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application." *Alice*, 573 U.S. at 217.

Patents granted by the Patent and Trademark Office are presumptively valid. *See, e.g., Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1319 (Fed. Cir. 2019). "Any fact, such as whether a claim element or combination is well-understood or routine, that is pertinent to the invalidity conclusion must be proven by clear and convincing evidence." *Id*. (cleaned up)*; see also Berkheimer v. HP Inc.*, 881 F.3d 1360, 1369 (Fed. Cir. 2018). And on a Rule 12 motion, the Court must accept as true Cortex's well-pleaded allegations with respect to whether its patents operate in a way that is plausibly inventive. *Cellspin,* 927 F.3d at 1319-20. "[P]atent eligibility may be resolved at the Rule 12 stage only if there are no plausible factual disputes after drawing all reasonable inferences from the intrinsic and Rule 12 record in favor of the non-movant." *Coop. Ent., Inc. v. Kollective Tech., Inc.,* 50 F.4th 127, 130 (Fed. Cir. 2022) (citing cases).

A. Cortex's Patents Are Directed to Specific Improvements in the Security and Fragmentation of Digital Transactions.

At step one of *Alice*, the Court analyzes "the language of the Asserted Claims themselves, considered in light of the specification." *TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278, 1292 (Fed. Cir. 2020). The Court looks to "the focus of the claimed advance over the prior art to determine if the claim's character as a whole is directed to excluded subject matter." *Koninklijke KPN N.V. v. Gemalto M2M GmbH*, 942 F.3d 1143, 1149 (Fed. Cir. 2019). In doing so, the Court must "articulate what the claims are directed to with enough specificity to ensure the step one inquiry is meaningful." *Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.*, 880 F.3d 1356, 1361 (Fed. Cir. 2018). The Supreme Court has recognized that "all inventions at some level embody, use, reflect, rest upon, or apply ... abstract ideas." *Mayo Collaborative Servs. v. Prometheus Labs., Inc*., 566 U.S. 66, 71 (2012). Thus, inventions which apply an abstract concept "to a new and useful end" remain eligible for patent protection. *Alice*, 573 U.S. at 217 (cleaned up).

"In cases involving authentication technology, patent eligibility often turns on whether the claims provide sufficient specificity to constitute an improvement to computer functionality itself." *Universal Secure Registry LLC v. Apple Inc.*, 10 F.4th 1342, 1346 (Fed. Cir. 2021). Here,

the Asserted Claims are directed to specific improvements to a specific computer technology: virtual wallets. The invention is thus "necessarily rooted in computer technology in order to solve a specific problem in the realm of computer networks." *Packet Intelligence*, 965 F.3d at 1309 (quoting *SRI International, Inc. v. Cisco Systems, Inc.*, 930 F.3d 1295 (Fed. Cir. 2019)). The Asserted Claims protect against identity theft and fraud through the novel technique of generating a *secondary representative* credential that has been *verified* by the agency that issued the initial credential and is *tied* to a specific user device. Before Cortex's invention, mobile-wallet applications struggled to find user-friendly ways to transmit sensitive personal information, like credit card or drivers' license numbers. *See* Compl. ¶ 11. The OVER File system permits users to make mobile credit-card payments and merchants to verify users' credit-card information, without transmitting *any* sensitive personal information *or* having to communicate with the credit card company. The user and the merchant need only communicate with the OVER engine to verify that the user's underlying credential is valid, a process that is instantaneous. This process is summarized in Figure 3 of the '531 Patent. '531 Patent at Sheet 3 of 12.

The OVER File system—which uses an officially verifiable electronic representation of a credential for use on a mobile device—cannot be implemented by hand or by "pen and paper methodologies." *See* Mot. at 13. Unlike the system for inputting bedside patient information in *Univ. of Florida Research Foundation., Inc. v. General Electric Co.*, 916 F.3d 1363, 1367 (Fed. Cir. 2019), Cortex's system is directed to, and requires, computers. Visa knows this. On July 24, 2023—mere weeks after Cortex first presented its technology to CyberSource—Visa applied for a patent entitled "Systems and Methods for Communicating Token Attributes Associated with a Token Vault." Brook Decl., Ex. 1. Like Cortex's '531 patent, that application called for an *electronic* computerized system "to request generation, use and management of tokens." *Id.* at 1.

The Federal Circuit has held that patent claims like these—directed to specific improvements to computer functionality—are patent-eligible under step 1 of *Alice. Enfish, LLC v. Microsoft Corp*., 822 F.3d 1327, 1336 (Fed. Cir. 2016). As the Federal Circuit has repeatedly recognized, "[i]mproving security . . . can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer

problem." *Ancora Techs., Inc. v. HTC Am., Inc.,* 908 F.3d 1343, 1348 (Fed. Cir. 2018); *see also CosmoKey Sols. GmbH & Co. KG v. Duo Sec. LLC*, 15 F.4th 1091, 1097 (Fed. Cir. 2021).

In *Ancora Technologies*, for example, the Federal Circuit held claims to be patent-eligible at step one when they provided new methods for preventing a computer from running unauthorized software. 908 F.3d at 1344. The Federal Circuit concluded that the claims addressed a specific technological problem affecting computers—the "vulnerability of license-authorization software to hacking"—by placing the license-authorization software in a less vulnerable portion of the computer's memory. *Id.* at 1348–49. Similarly, in *Finjan*, the Federal Circuit held that claims for a new method of virus scanning were patent-eligible at step one. 879 F.3d at 1302. By undertaking a "behavior-based approach" to virus scanning rather than a traditional "code-matching" approach, the claims at issue in *Finjan* comprised "a new kind of file that enable[d] a computer security system to do things it could not do before." *Id.* at 1304–05.

Like the claims in *Ancora Technologies* and *Finjan*, the Asserted Claims provide a new data structure that departs from earlier approaches to solve known problems affecting electronic transactions—namely the challenges of storing and transmitting sensitive personal information on a mobile device used in mobile transactions. Cortex invented a virtual intermediary, the OVER Engine, that eliminates traditional third-party middlemen like banks and other credential-issuing agencies from digital transactions. Just as the claims in *Ancora Technologies* provided for the unique placement of license-authorization software within a computer's memory that made hacking more difficult, the Asserted Claims create a remote OVER Engine to store a user's sensitive personal information instead of on the user's device and verify the user's credentials through the OVER Engine rather than at the point-of-sale, e.g., by a third-party credential-issuing agency or a bank. The only credential stored on a user's device is a *meta representation* of the original credential. And just like the claims at issue in *Finjan*, which described a novel, behavior-based approach to virus scanning that made the computer more secure than with preexisting software, the Asserted Claims detail a novel structure—in which parties to a transaction communicate using a secondary credential that is verified by an intermediary database (the OVER Engine) without ever having to communicate with the original credential issuing agency—that

makes electronic transactions less susceptible to identity theft than preexisting techniques. Like the self-referential database deemed patent-eligible in *Enfish*, the OVER File system "functions differently than conventional [data] structures" by routing all point-of-sale communications through the remote OVER Engine. 822 F.3d at 1337. Before Cortex's invention, a user could not make a purchase with a mobile device without storing her credential on her phone, displaying her credential to a third party, *and* requiring that third party to communicate with the issuing agency.

Visa, unable to address these precedents regarding specific enhancements to computer security and authentication, instead attempts to reduce the Asserted Claims to the purportedly abstract idea of "issuing and checking credentials" or "verification of credentials by a centralized authority." Mot. at 9-10, 13. Those arguments ignore the *representative* nature of the OVER File system and the Asserted Claims' plain focus on virtual wallets. They are also wrong as a matter of law. "[D]escribing the claims at such a high level of abstraction and untethered from the language of the claims all but ensures that the exceptions to § 101 swallow the rule." *Enfish*, 822 F.3d at 1337; *see also, e.g.*, *CardioNet, LLC v. InfoBionic, Inc.*, 955 F.3d 1358, 1371 (Fed. Cir. 2020) ("Generalizing the asserted claims as being directed to collecting, analyzing, and reporting data is inconsistent with our instruction that courts be careful to avoid oversimplifying the claims by looking at them generally and failing to account for the specific requirements of the claims.").

Visa commits that very error by characterizing the Asserted Claims as "nothing more than the longstanding activity" of the Department of Motor Vehicles verifying driver's licenses through driver's license numbers or universities authenticating the validity of diplomas and transcripts. Mot. at 10. To arrive at this characterization, Visa "had to disregard elements of the claims at issue that the specification makes clear are important parts of the claimed advance in the combination of elements." *TecSec,* 978 F.3d at 1294. For example, Visa ignores the specific improvements of Cortex's patents on the very processes that it describes. Consider Visa's DMV example. The OVER File system obviates the need for a user to carry her driver's license number, which is exploitable personal information, on her phone, or to share this number with a third-party seeking verification. Instead, the user need only share a verifiable electronic representation of that license. And the third-party verifier need not communicate with the DMV or any other

"central authority" to verify the user's license information. Instead, the verifier need only scan the user's OVER File receive a verification notice from the OVER File engine. Cortex's patents permit two parties to verify user credentials without either sharing personal information or communicating directly with a third-party issuing agency.

Visa's analogies are also inconsistent with precedent. In *Ancora Technologies*, for example, the Federal Circuit "held the claims at issue to be directed to solving a problem presented by particularly easy unauthorized use of software by placing the software in an especially secure computer location, even though placing items in especially secure locations to prevent unauthorized access is a goal in many settings." *TecSec*, 978 F.3d at 1296 (citing *Ancora Techs.*, 908 F.3d at 1349). The same is true here: while non-electronic transactions may implicate the security of personal information, that does not negate the conclusion that the patents are aimed at solving "particular problem[s]" that are unique to the storage of credentials and conducting electronic transactions *on mobile devices*. *Id; see also DDR Holdings, LLC v. Hotels.com, L.P.,* 773 F.3d 1245, 1257 (Fed. Cir. 2014) ("Although the claims address a business challenge (retaining website visitors), it is a challenge particular to the Internet.").

Unlike the cases cited by Visa, Cortex's patents do not simply utilize[] a computer generally as a tool to conduct a known or obvious process." *Smart Authentication IP, LLC v. Elec. Arts Inc.*, 402 F. Supp. 3d 842, 850 (N.D. Cal. 2019). In *Smart Authentication,* the Court found ineligible a patent for multi-factor authentication of users over multiple communications media as an obvious combination of two abstract ideas: "the use of a third party intermediary to confirm the identity of a participant to a transaction and the use of a temporary code to confirm the identity of a participant to a transaction." *Id.* The similar patent in *Prism Technologies LLC v. T-Mobile USA, Inc.*, 696 Fed. App'x 1014 (Fed. Cir. 2017) was ineligible for the same reasons. As were the patents in *Secured Mail Solutions. LLC v. Universal Wilde, Inc.*, 873 F.3d 905, 907 (Fed. Cir. 2017), which merely called for the use of "intelligent" barcodes to authenticate pieces of mail. Cortex's patents, by contrast, disclose a new data structure which far surpasses the simplicity of using a temporary authorization code to confirm a participant's identity—by creating a *secondary electronic credential* that is stored on a user's phone with all the

functionality of the primary credential but none of the risk associated with storing or transmitting sensitive information, and that is verifiable without having to contact the issuing agency.

For that reason, the Asserted Claims are also distinguishable from the patents in *Universal Secure Registry*, which described a method in which a user submits a "one-time code" to a merchant, which then transmits that code and the amount of purchase to the credit-card company, which in turn submits the code to a "Universal Secure Registry," and the registry communicates the credit card number back to the credit card company. Cortex's invention not only calls for the generation of a less transient and reusable representative credential, but also also obviates the need for the merchant to communicate with the credit card company at all, or for any credit card information to be communicated at the point-of-sale. 10 F.4th at 1348. Indeed, Cortex's OVER File system frees each party to a transaction from unnecessary communication cycles with various third parties, requiring only a single ping from a user device to the OVER Engine, which provides a response. All OVER Files generated by the OVER Engine have been verified by the issuing agency *before* the transaction begins. Unlike the generation of a one-time authentication code, the generation of a secondary electronic representation of a user credential is neither "conventional" nor "long-standing." *Id.* at 1350. Cortex's method aims specifically at improving the privacy and security of digital transactions using virtual wallets.

B. Cortex's Patents Supply Inventive Concepts for Enhancing the Security and Interoperability of Electronic Transactions

Even if the Court were to find the Asserted Claims to be directed to an abstract idea, they would nonetheless be patent-eligible at step two of *Alice*. At step two, the Court searches for an "inventive concept" that is "sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself." *Alice*, 573 U.S. at 217–18. Step two is satisfied "when the claim limitations involve more than performance of well-understood, routine, and conventional activities previously known to the industry." *Berkheimer*, 881 F.3d at 1367. The Federal Circuit has held that even if individual elements of a claim are generic or conventional, the claims are patent-eligible when the ordered combination of elements provides a technical improvement over the prior art. *See, e.g., Bascom Glob. Internet Servs., Inc. v. AT&T Mobility*

LLC, 827 F.3d 1341, 1350 (Fed. Cir. 2016) (claims found eligible even though individual elements were generic computer and network components, because there was "an inventive concept … in the non-conventional and non-generic arrangement of [the] known, conventional pieces").

Here, beyond parroting case law, Visa never attempts to carry its burden to *show*—with evidence—why each claim limitation taught by the Asserted Claims is well-understood, routine, or conventional or otherwise not inventive. *See Aatrix Software, Inc. v. Green Shades Software, Inc.*, 890 F.3d 1354, 1356 (Fed. Cir. 2018) (Moore, J., concurring in the denial of rehearing en banc) ("Because the patent challenger bears the burden of demonstrating that the claims lack patent eligibility, 35 U.S.C. § 282(a), there must be evidence supporting a finding that the additional elements were well-understood, routine, and conventional."). That is because it cannot.

Visa attempts to muddle the step two inquiry by isolating parts of the claims and arguing that those parts—standing alone—do not supply an inventive concept. *See, e.g.*, Mot. at 13-14. But "[t]he inventive concept inquiry requires more than recognizing that each claim element, by itself, was known in the art" because "an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces." *Bascom*, 827 F.3d at 1350. Even assuming that the claims are directed towards the abstract idea of "issuing and verifying credentials," they disclose an inventive concept by the ordered combination of the limitations.

First, they teach storing the sensitive personal information of a user credential on a remote database, rather than on the user's mobile phone, contrary to the state of the art as of the '531 patent's priority date of December 21, 2012. *See* Compl. ¶ 8. The security advantages of this approach are plain, namely protecting sensitive information from would-be hackers of mobile devices. Second, the Asserted Claims teach the generation of a secondary representative credential that has all the functionality of an original credential but without the sensitive personal information intact. This secondary credential allows users to carry on their phones a "virtual wallet platform [that] may provide electronic replacement for credit cards, cash, identification or other cards traditionally carried in a wallet." '854 patent at 9:66-10:2. Moreover, Cortex's patents disclose the inventive concept of linking the OVER File to a specific user device. As described in

the specification, "[t]the OVER File credential may only be usable by a device matching the device or application identifier. By tying the OVER File credential to a specific device, the security of the credential is increased, as an OVER File delivered to a device other than the user device, for example through network snooping, may be prevented from working on a device other than the user device." '531 Patent at 7:14-20. Third, the Asserted Claims allow a third-party to scan the secondary credential from the user's mobile device and obtain authentication without having to communicate with the issuing agency. Cortex's patents additionally permit a user to display the secondary credential without risk that *either* the secondary credential *or* the original credential with sensitive information will be duplicated, by disabling all device functions (such as screenshots) while the credential is displayed on a user's screen. *Id.* at 13:58-64. Those limitations, as the common specification explains and as enumerated in the Complaint, were neither well-understood, routine, nor conventional in 2012.

The Federal Circuit's decision in *CosmoKey Solutions* is instructive. There, the patent at issue concerned a dual-factor authentication system, *i.e.*, a means of verifying the identity of a user performing a transaction on a terminal (such as a computer) by activating an authentication function on the user's mobile phone. 15 F.4th at 1093. In holding that the claims were patent eligible at step two of *Alice*, the Federal Circuit rejected the district court's conclusion that the claims "merely t[aught] generic computer functionality to perform the abstract concept of authentication." *Id.* at 1095; *see* Mot. at 13–14 (pressing similar arguments). Rather, the claims at issue in *CosmoKey Solutions* recited specific steps—including "ensuring that the authentication function is normally inactive, activating only for a transaction, communicating the activation within a certain time window, and thereafter ensuring that the authentication function is automatically deactivated"—that enhanced "computer and network security." 15 F.4th at 1099. Cortex's claims are likewise eligible at step two of *Alice* because they recite specific steps, including the generation, transmission, and verification of an OVER File, and the scanning by a third-party of a displayed portion of an OVER file on a mobile device, which in combination enhance security in transactions carried out on mobile phones.

Visa tries to sidestep the inventive-concept inquiry by mischaracterizing Cortex's

allegations as wholly preempting the alleged abstract idea of "provisioning a *representative* credential, that can be scanned and verified," Mot. at 13 (emphasis added). Even if provisioning a *representative* credential *does* comprise an abstract idea (or the appropriate level of abstraction to be used in an *Alice* analysis), Cortex's invention does not preempt the concept. It is true that the Asserted Patents create a system that covers every aspect of conducting transactions using representative credentials—from storage, to generation, to transmission, to verification, to authentication. But it is only that particular system, detailed over numerous specific limitations in multiple patents, that is patented.

Visa fares no better by characterizing the claims as being "written in functional language," Mot. at 13. Even if the claims did employ "functional, result-based language," "the language of the claim and the specification are directed to more than just these results." *See Broadcom Corp. v. Netflix Inc.*, 2021 WL 4170784, at *12 (N.D. Cal. Sept. 14, 2021). Numerous cases with materially indistinguishable language upholding patent eligibility confirm that the use of "functional language" in claims, standing alone, does not render claims ineligible. *Finjan* upheld a method comprising "*receiving* . . . a Downloadable," "*generating* . . . a security profile that identifies suspicious code in the received Downloadable," and "*linking* . . . the . . . security profile to the Downloadable before a web server makes the Downloadable available to web clients." 879 at 1303–04. *SRI* upheld a method comprising "*deploying* a plurality of network monitors," "*detecting* . . . suspicious activity," "*generating* . . . reports of said suspicious activity," and "automatically *receiving* and *integrating* the reports of suspicious activity." 930 F.3d at 1301. Even Visa's own "token vault" patent employs the same functional language. *See* Brook Decl., Ex. 1 at 60.

Nor is it dispositive that the invention is implemented on "only generic computer functionality." Mot at 13. The patent in *Bascom*'s reliance on generic computer and network components, did not preclude it from disclosing an inventive concept under *Alice*. 827 F.3d at 1349–50 ("[T]he limitations of the claims, taken individually, recite generic computer, network and Internet components, none of which is inventive by itself."). As explained above, the Asserted Claims disclose inventive steps beyond the well-understood, routine, or conventional.

C. Disputed Factual Issues Preclude Judgment on the Pleadings.

"[P]atent eligibility is ultimately a question of law." *Berkheimer*, 881 F.3d at 1367. But the inquiry is "rife with underlying factual issues." *Ultramercial, Inc. v. Hulu, LLC*, 722 F.3d 1335, 1339 (Fed. Cir. 2013), *vacated on other grounds*, 573 U.S. 942 (2014). "Whether something is well-understood, routine, and conventional to a skilled artisan at the time of the patent is a factual determination." *Berkheimer*, 881 F.3d at 1369. Here, at the very least, there are disputed issues of fact regarding whether the Asserted Patents teach methods that were not "well-understood, routine, or conventional." That precludes judgment on the pleadings.

Patents are presumptively eligible. Subject matter ineligibility is an affirmative defense to infringement that the *defendant*—not Cortex—must prove by clear and convincing evidence. *Cellspin*, 927 F.3d at 1319; 35 U.S.C. § 282. And for affirmative defenses generally, it is black-letter law that the *defendant* must plead them. *See* Fed. R. Civ. P. 8(c); *Barnes v. AT&T Pension Ben. Plan-Nonbargained Program*, 718 F. Supp. 2d 1167, 1171 (N.D. Cal. 2010). To be sure, the Federal Circuit has explained that "patentees who adequately allege their claims contain inventive concepts survive a § 101 eligibility analysis under Rule 12(b)(6)." *Cellspin*, 927 F.3d at 1318. But *Cellspin* establishes a *sufficient* condition for defeating 12(b)(6) motions, not a *necessary* condition requiring plaintiffs to plead eligibility. There is no reason why a § 101 defense should be treated differently from any other affirmative defense. To the extent that the Court is inclined to find that Cortex was required to plead that the patents each teach "an inventive concept," Cortex requests the opportunity to amend its pleadings.

II. Cortex Adequately Alleges Willful and Indirect Infringement

The Complaint that Cortex served on Visa nearly a year ago provided Visa with sufficient notice of the Asserted Patents and its allegations of infringement. Visa incorrectly argues that Cortex must allege that Visa had *pre-suit* knowledge of its patents in order for Cortex to sustain claims for *post-suit* willful and induced infringement. Mot. at 7-8, 14-15. That minority view runs contrary to a robust consensus of authority on the subject and to the purposes of the Patent laws. The Federal Circuit has found that claims of indirect infringement were sufficient where they

alleged that defendants were aware of the patent when served with the complaint. *See In re Bill of Lading*, 681 F.3d at 1344. A majority of Courts in the Ninth Circuit agree, and for good reason:

> "A defendant should not be able to escape liability for postfiling infringement when the complaint manifestly places the defendant on notice that it allegedly infringes the patents-in-suit. Holding otherwise would give a defendant carte blanche to continue to indirectly infringe a patent—now with full knowledge of the patents-in-suit—so long as it was ignorant of the patents prior to being served itself with the complaint. This strange reward would quickly erode the foundation upon which Congress constructed § 271(b) and (c)'s liability structure."

MyMedicalRecords, Inc. v. Jardogs, LLC, 1 F. Supp. 3d 1020, 1025 (C.D. Cal. 2014); *accord Teradyne, Inc. v. Astronics Test Sys., Inc.,* 2020 WL 8173024, at *5 (C.D. Cal. Nov. 6, 2020); *Parity Networks, LLC v. Moxa Inc.*, 2020 WL 6064636, at *5 (C.D. Cal. Sept. 11, 2020); *Symantec Corp. v. Veeam Software Corp.*, 2012 WL 1965832, at *4 (N.D. Cal. May 31, 2012); *see also CAP Co. v. McAfee, Inc.*, 2015 WL 3945875, at *5 (N.D. Cal. June 26, 2015) ("A complaint is a perfectly adequate notice to defendants for indirect infringement claims for post-filing conduct."). This Court has also adopted that view. *NetFuel, Inc. v. Cisco Sys. Inc.*, 2018 WL 4510737, at *3 (N.D. Cal. Sept. 18, 2018) ("Plaintiff's complaint certainly provides the Defendant with notice of the Patents-in-Suit and their allegations of infringement.").

A. Cortex Adequately Alleges Pre-Suit Willful Infringement of the '531 Patent

To state a claim for willful infringement, a plaintiff must allege facts plausibly showing that the defendant 1) had "knowledge of the patent alleged to be willfully infringed" and 2) "engaged in deliberate or intentional infringement." *Core Optical Techs., LLC v. Juniper Networks Inc*., 562 F. Supp. 3d 376, 381 (N.D. Cal. 2021) (cleaned up). "[S]ubjective willfulness" can be shown by "proof that the defendant acted despite a risk of infringement that was 'either known or so obvious that it should have been known to the accused infringer.'" *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc*., 876 F.3d 1350, 1371 (Fed. Cir. 2017) (quoting *Halo Elecs., Inc. v. Pulse Elecs., Inc.*, 579 U.S. 93, 105 (2016)).

Cortex's allegations of pre-suit willful infringement of the '531 patent meet this standard. Cortex explained the '531 Patent to two different Visa executives on two separate occasions. In both instances, Cortex provided Visa with a detailed description of its OVER File technology and alerted Visa that Cortex had been issued a patent for that same technology. Compl. ¶ 11. The

documents clarified that Cortex's patent encompassed the entirety of the tokenization process described. *See id.* (describing Cortex's IP as "covering every aspect of provisioning a representative credential, that can be scanned and verified").

There can be no doubt that these communications alerted Visa of the potential that its token service infringed the patent discussed. Cortex informed Visa that its OVER File IP related directly to *that product Id.* ¶ 11. Cortex also expressly alerted Visa that its OVER File patent was being infringed by "most all" providers of wallet solutions on the market.[3] *Id.* And the express purpose of those communications was to explore a commercial relationship between Cortex and Visa based on Cortex's "[c]ritical supporting IP portfolio." *Id.* The connection between the OVER File patent and the Visa Token Service was apparent from the context of the 2016 conversations: the Visa executive involved was the person responsible for the Visa Token Service product. *Id.* The substance of these disclosures, which were made to two different Visa executives on two occasions within a year, make it reasonable to infer that Visa knew, or at the very least should have known, that the Visa Token Service was infringing Cortex's '531 Patent.

Visa argues that these representations were insufficient to place Visa on notice of infringement because Cortex did not provide Visa with a copy "of the '531 patent," Mot. at 15, or "accuse[] Visa of infringement," *id.* at 16. Yet Visa does not offer any caselaw supporting its proposition that the absence of patent numbers, claim language, or infringement accusations is fatal to a claim of willful infringement. That is because the law imposes no such requirement.

To the contrary, this precise argument was recently rejected in *Mobile Equity Corp. v. Walmart Inc*, 2022 WL 4587554 (E.D. Tex. Sept. 8, 2022), *report and recommendation adopted*, 2022 WL 4587499 (E.D. Tex. Sept. 27, 2022). The *Mobile Equity* court rejected the argument that a presentation given by the patentee to defendant Walmart "neither included a copy of the

[3] Visa argues that "Wallet Solution" is an obscure or undefined concept. Mot. at 17. In fact, it is a commonly understood term in the payments world that Visa itself uses. Visa's website page about digital wallets includes a section called "Build Your Own Wallet Solution." which notes that the relevant issuer "needs to be a participant in the Visa Token System." https://partner.visa.com/site/explore/digital-wallets.html. The Complaint also alleges that Cortex's OVER File technology is a "mobile-wallet solution" and explains how Cortex's tokenization technology fits into the existing world of wallet solutions. Compl. ¶¶ 8-9.

Asserted Patents or identifying patent numbers, offered a license, or accused Walmart of infringement." *Id.* at *2. Instead, the court concluded that the "presentation [that] described the technology of the Asserted Patent" and "disclosed the technology's status as patented in the United States" at a time when Walmart was "actively rolling out and deploying the accused service" was sufficient *at the summary judgment stage* "to establish a genuine dispute of material fact regarding Walmart's actual knowledge of or willful blindness to infringement of the [Asserted] Patent." *Id.* at *3. As here, those discussions took place in the context of a potential business relationship. *See id.* at *2. Cortex's allegations of each of the above facts are sufficient to withstand the lower plausibility standard applicable to this motion.

Visa's caselaw is distinguishable because in Visa's cases plaintiffs did not allege that they had placed defendants on notice of the connection between the asserted patents and the accused products. In *Michigan Motor Techs. LLC v. Volkswagen Aktiengesellschaft*, 472 F. Supp. 3d 377 (E.D. Mich. 2020), plaintiff "wrote only one sentence in support of willfulness: 'Defendants were made aware of the patents-in-suit at least as early as March 4, 2015, when [they were] provided notice of the patents via letter.'" *Id.* at 384. Unlike the allegations here, plaintiffs "never specified what the letter stated, did not mention who sent the letter, and did not mention to whom the letter actually was sent." *Id.* Similarly, the alleged notice letter in *Bench Walk Lighting LLC v. LG Innotek Co.*, 530 F. Supp. 3d 468, 492 (D. Del. 2021) failed to reference not only the accused products but two of the patents alleged to be willfully infringed. A plaintiff need only plead sufficient facts to plausibly allege that the defendant knew, or should have known, that the conduct amounted to infringement. *Arctic Cat Inc.*, 876 F.3d at 1371. Unlike the "conclusory allegations" that the Court rejected in *WiNet Labs LLC v. Apple Inc.*, 2020 WL 409012, at *5 (N.D. Cal. Jan. 24, 2020), Cortex's allegations meet that standard: they identify by name the two Visa executives to whom Cortex disclosed information and in what context, and allege detailed facts about the contents of information disclosed. *See* Compl. ¶ 11.

B. Cortex Adequately Alleges Induced Infringement

To plead a claim for induced infringement, the plaintiff must show that the alleged inducer (1) knew of the patent, (2) knowingly induced the infringing acts, and (3) possessed a specific

intent to encourage another's infringement of the patent. *Vita–Mix Corp. v. Basic Holding, Inc.*, 581 F.3d 1317, 1328 (Fed. Cir. 2009). "Circumstantial evidence can support a finding of specific intent to induce infringement." *Vanda Pharm. Inc. v. W.-Ward Pharm. Int'l Ltd.*, 887 F.3d 1117, 1129 (Fed. Cir. 2018). An allegation that a party, upon having knowledge of the patent and the alleged infringing acts, provided instructions on how to use a product in an infringing manner is sufficient to show a specific intent to induce infringement. *See Microsoft Corp. v. DataTern, Inc.*, 755 F.3d 899, 905 (Fed. Cir. 2014).

First, as discussed above, Cortex's allegations, and the inferences reasonably drawn therefrom, adequately plead that Visa knew of the '531 Patent and knew or should have known that the Visa Token Service infringed that patent before service of Cortex's complaint. Moreover, even if Cortex's allegations of pre-suit knowledge of that patent were insufficient, Visa's complaint still alleges a viable claim for post-complaint indirect infringement for all of the Asserted Patents because Cortex's complaint put Visa on notice of the patents and their infringement. *See supra* pp. 17-18.

Second, intent can be sufficiently pled by allegations that an accused product infringes a patent, that the accused infringer is aware of the patent, and that the accused infringer instructs and encourages its customers to use that product. *See Bill of Lading*, 681 F.3d at 1341-45 (holding that plaintiff sufficiently pled the "intent" element of induced infringement claim with allegations that defendants, with knowledge of the patents, encouraged and instructed third parties to use patented invention). Specific intent is also satisfied by allegations that the defendant "provides software development kits that instruct and encourage the use of the infringing products, instructional support on its website, information and technical support on third-party platforms, and video instruction…." *IOENGINE, LLC v. PayPal Holdings, Inc.*, 2019 WL 330515, at *5 (D. Del. Jan. 25, 2019).

Cortex has pled sufficient facts to establish Visa's specific intent to induce infringement. As a preliminary matter, Cortex's complaint details how use of the Visa Token Service directly infringes each of the Asserted Patents. Compl. ¶¶ 18-25 ('531 Patent), ¶¶ 39-48 ('854 Patent), ¶¶ 62-68 ('859 Patent), ¶¶ 82-91. Visa does not challenge the adequacy of those allegations,

which make clear that any use of the Visa Token Service infringes the Asserted Patents. This is not a case in which the Accused Products can be used in a non-infringing manner. Cortex alleges three different ways in which Visa instructs banks, merchants, and developers on how to use this infringing service—through the Visa developer center, through the EMVCo technical specifications, and through CyberSource's token management service. *Id.* ¶¶ 27, 50, 70, 93. EMVCo evidently recognizes that implementation of its instructions may infringe the patent rights of third parties, as it appended a disclaimer of liability to its tokenization use guide. *See id.* ¶ 27. Cortex further alleges that Visa provides software development guides, tutorials, and webinars that teach those same third parties how to implement the Visa Token Service. Visa's publication of specific instructions distinguishes its conduct from the allegations in *Fluidigm Corp. v. IONpath, Inc.*, 2020 WL 408988, at *4 (N.D. Cal. Jan. 24, 2020) in which the plaintiff pointed only to "brochures" encouraging the patented practice. Cortex's allegations are sufficient to state a claim for indirect infringement. *See, e.g.*, *Bill of Lading*, 681 F.3d at 1341-45; *Microsoft Corp.*, 755 F.3d at 905; *IOENGINE, LLC*, 2019 WL 330515, at *5.

Visa cites a litany of inapposite cases, *see* Mot. 19-20, but the "generalized allegations" found insufficient in those allegations are nothing like the specific facts alleged in Cortex's Complaint:

- In *Addiction & Detoxification Inst. L.L.C. v. Carpenter*, 620 F. App'x 934 (Fed. Cir. 2015), the complaint "contain[ed] no allegations regarding intent or any specific acts caused by Defendants" to support its indirect infringement claims. *Id.* at 938.

- In *CyWee Grp. Ltd. v. HTC Corp.*, 312 F. Supp. 3d 974, 980 (W.D. Wash. 2018) the complaint asserted that Defendant "continued to create and disseminate product manuals, instructions, and marketing materials" but offered "no specific details about those promotional and instructional materials." Here, Cortex provides links to and quotes from numerous such examples.

- In *Michigan Motor Techs. LLC v. Volkswagen Aktiengesellschaft*, 472 F. Supp. 3d 377 (E.D. Mich. 2020), the complaint included only conclusory allegations about defendants' "distributing the Accused Instrumentalities and providing materials and/or services related to the Accused Instrumentalities" with no more detail. *Id.* at 385. It also suffered from a "lack of pleaded facts"—even circumstantial—"that might show specific intent," asserting only that "defendants induced others to infringe MMT's patents 'with specific intent' to do so, 'or with willful blindness to the resulting infringement.'" *Id.* at 386. Once again, Cortex's detailed allegations are nothing like the threadbare recitations in *Michigan Motor*.

Cortex's allegations of induced infringement are entirely connected to the claims of the Asserted Patents, despite Visa's arguments to the contrary. *See* Mot. at 20. Visa cites *Memory Integrity LLC v. Intel Corp.*, 144 F. Supp. 3d 1185, 1195 (D. Or. 2015), for the proposition that, "[w]here defendants have not touted the benefits of the accused products in ways that track the asserted patents, courts generally do not infer specific intent." Mot at 20. But the Federal Circuit has rejected such a strict requirement for indirect infringement. *See Bill of Lading*, 681 F.3d at 1341-42 (rejecting defendant's argument that plaintiff had "not provided statements from [defendant] which specifically instruct [defendant's] customers to perform all of the steps of the patented method," because "[defendant] is essentially arguing that, at the pleading stage, [plaintiff] must allege facts that prove all aspects of its claims, or at the very least make those claims probable. But that is not what is required."). "[T]here is no requirement that the facts alleged mimic the precise language used in a claim; what is necessary is that facts, when considered in their entirety and in context, lead to the common-sense conclusion that a patented method is being practiced." *Id.* at 1343.

The facts alleged by Cortex mandate such a conclusion. Take the example of EMVCo. Visa claims that that Cortex does not allege any "specific portion of [the EMVCo specifications or user guide] to any specific claim of any of the Asserted Patents." Mot at 21. Not so. In fact, Cortex specifically alleges that multiple EMVCo specifications—each of which is contained in a user guide intended to encourage third-party implementation of tokenization—track multiple claims in *each* of the Asserted Patents. *See* Compl. ¶¶ 22, 23 ('531 patent); *id.* ¶¶ 39, 41, 42, 43, 44, 48 ('854 patent); *id.* ¶¶ 63, 65, 66, 67 ('859 patent); *id.* ¶¶ 82, 83, 84, 87, 88 ('973 patent). Each of the aforementioned allegations cites to either the EMVCo Specification Technical Framework or Guide to Use Cases. And each alleges that Visa Token Service implements the specifications published by EMVCo in infringement of the relevant patent. In other words, Cortex's complaint *does* "specify which EMVCo processes VTS implements, and which of those process, if any, purportedly infringe the Asserted Patents," Mot. at 22.

Visa fares no better in attempting to sever its connection with EMVCo. Mot. at 22. Cortex has alleged sufficient facts to draw the reasonable inference that Visa acts through EMVCo. In

addition to the specific allegations described above, Cortex alleges that the Visa Token Service implements the tokenization process published by EMVCo and that Visa follows EMVCO's published specifications for tokenization. Compl. ¶ 16. Cortex has further alleged that Visa founded, manages, and has an ownership stake in EMVCo. *Id.* ¶ 16.

Lastly, Visa argues that Cortex's citation to mere instructions does not adequately plead the encouragement required by indirect infringement. Mot at 20 (citing *Takeda Pharms. U.S.A., Inc. v. W.-Ward Pharm. Corp.*, 785 F.3d 625 (Fed. Cir. 2015). *Takeda Pharmaceuticals* stated that inducement is found where instruction manuals indicate the product should be used in an infringing manner. *Id.* at 631. Here, Cortex has alleged that the Visa Token Service has no substantial non-infringing use. Unlike the "off-label" infringing use of drugs at issue in *Takeda Pharmaceuticals*, use of the Visa Token Service inherently infringes the Asserted Patents. Moreover, Cortex has alleged that Visa encourages software developers to implement its tokenization programs and provides webinars to aid in implementation. *See IOENGINE,* 2019 WL 330515, at *5 (finding specific intent satisfied where the plaintiff alleged that the defendant "provides software development kits that instruct and encourage the use of the infringing products, instructional support on its website, information and technical support on third-party platforms, and video instruction…").

C. Cortex Adequately Alleges Contributory Infringement

"Contributory infringement occurs if a party sells, or offers to sell, 'a component of a patented ... combination, ... or a material ... for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use.'" *Nalco Co. v. Chem-Mod, LLC*, 883 F.3d 1337, 1356 (Fed. Cir. 2018) (quoting 35 U.S.C. § 271(c)). "Contributory infringement requires knowledge of the patent in suit and knowledge of patent infringement," but a plaintiff need not plead intent to state a claim for contributory infringement. *Id.* (quoting *Commil USA, LLC v. Cisco Sys., Inc.*, 575 U.S. 632, 640, (2015)). "The Federal Circuit has ruled that affirmatively pleading the absence of substantial non-infringing uses renders the claim plausible if the pleadings do not undermine that allegation."

Merck Sharp & Dohme Corp. v. Teva Pharm. USA, Inc., 2015 WL 4036951 at *7 (D. Del. July 1, 2015) (citing *Bill of Lading*, 681 F.3d at 1339).

These cases demonstrate the soundness of Cortex's allegations of contributory infringement and contradict any argument that they should be dismissed as boilerplate recitation of the claim's elements. *See* Mot. 23. Unlike the allegations in *Bill of Lading,* Cortex's complaint does not "make clear on [its] face that [defendant's] products *do* have substantial non-infringing uses," 681 F.3d at 1339 (emphasis in original).[4] To the contrary, Cortex has alleged that the processes implemented by the Visa Token Service chart directly on the claims in the Asserted Patents. Compl. ¶¶ 18-25 ('531 Patent), ¶¶ 39-48 ('854 Patent), ¶¶ 62-68 ('859 Patent), ¶¶ 82-91. Cortex has further alleged that the infringing aspects of the Visa Token Service have no meaningful use other than in payment tokenization, and therefore no meaningful non-infringing use. *Id.* ¶¶ 31, 54, 74, 97; *cf. Traxcell Techs., LLC v. Verizon Wireless Pers. Commc'ns, LP*, 2022 WL 299732, at *5 (W.D. Tex. Jan. 31, 2022) (dismissing claims of contributory infringement because complaint failed to even *allege* that the accused products have no substantial non infringing uses). In sum, the Visa Token Service "can perform the infringing method and *only* the infringing method." *Bill of Lading*, 681 F.3d at 1338. Cortex's detailed allegations regarding the functionality of the Accused Products, "particularly allegations supporting the inference they the only have one purpose," namely a file format and platform for storage and verification of credentials," are sufficient to establish the lack of a substantial noninfringing use. *ScaleMP, Inc. v. TidalScale, Inc.*, 2019 WL 7877939, at *5 (N.D. Cal. Mar. 6, 2019). Visa has identified no potential non-infringing use of the Visa Token Service. Those allegations are thus sufficient to plead a claim for contributory infringement.

CONCLUSION

For the foregoing reasons, Visa's motion to dismiss should be denied in its entirety.

[4] Visa's reliance on *BlackBerry Ltd. v. Nokia Corp.*, 2018 WL 1401330 (D. Del. Mar. 20, 2018) is misplaced. In *BlackBerry,* the court dismissed claims for contributory infringement because plaintiff attempted to charge various foreign Nokia entities with contributory infringement based on the parent-subsidiary relationship with Nokia's U.S. entity without providing any factual basis to infer that the foreign entities knew of the actions of their U.S. subsidiary.

DATED: February 5, 2024

Respectfully submitted,

SUSMAN GODFREY L.L.P.

By: */s/ Kalpana Srinivasan*

Kalpana Srinivasan State Bar No. 237460
Davida Brook State Bar No. 275370
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, 14th Floor
Los Angeles, California 90067-6029
Telephone: (310) 789-3100
Fax: (310) 789-3150
ksrinivasan@susmangodfrey.com
dbrook@susmangodfrey.com

Max L. Tribble, Jr. State Bar No. 326851
Bryce Barcelo (pro hac vice forthcoming)
SUSMAN GODFREY L.L.P.
1000 Louisiana Street, Suite 5100
Houston, Texas 77002-5096
Telephone: (713) 651-9366
Fax: (713) 654-6666
mtribble@susmangodfrey.com
bbarcelo@susmangodfrey.com

Tyler Finn (pro hac vice forthcoming)
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, New York 10019
Telephone: (212) 336-8330
Fax: (212) 336-8340
tfinn@susmangodfrey.com

Attorneys for Plaintiff Cortex MCP, Inc